1. Extensions Determined by Split Primes

Let L/K be a finite extension of number fields, not necessarily Galois. Let S be a finite (or density zero) set of primes of K. Let $\mathrm{Spl}_S(L/K)$ be primes $v \notin S$ that split completely in L. Let $\mathrm{Spl}'_S(L/K)$ be the set of primes $v \notin S$ such that v has a split factor in L.

1.1. Dirichlet density.

A place $w|v$ is split if and only if $\mathrm{Fr}_w = 1$. Thus

$$\mathrm{Spl}_S(L/K) = \{v | v \notin S, \forall w, \mathrm{Fr}_w = 1 \in G(L/K)\}.$$

By the Chebotarev density theorem, this set corresponds to the conjugacy class of the identity. Thus, its density is $1/[L:K]$.

1.2. Split Primes Determine Extension.

Suppose for L, M Galois extensions over K, we have the relation $\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K)$. Then if $L \subset M$, $LM = M$ and so $\mathrm{Spl}_S(M/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K)$. Then $\mathrm{Spl}_S(M/K) \subset \mathrm{Spl}_S(L/K)$. If we start with this, we can conclude $\mathrm{Spl}_S(M/K) = \mathrm{Spl}_S(LM/K)$. Thus, in the extension LM/M, no new primes split. Since L/K is Galois, LM/M is a Galois extension. By the previous part, this cannot happen for a non-trivial extension since the set of completely split places has positive density. Thus, $LM = M$, or $L \subset M$.

1.2.1. *Splitting in a Composite Field.*

It remains to verify the relation. Due to transitivity of ramification indices and inertial degrees, it is clear that $\mathrm{Spl}_S(LM/K) \subset \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K)$. Now take a place v in the right hand side. Note that $L, M \otimes_K K_v \cong K_v^{[L:K],[M:K]}$ respectively, due to the totally split condition. It is not hard to see that there is a surjective map of K_v-algebras

$$(L \otimes_K K_v) \otimes_{K_v} (M \otimes_K K_v) \to LM \otimes_K K_v,$$

given by $(a \otimes b) \otimes (a' \otimes b') \to aa' \otimes bb'$. Since $LM \otimes_K K_v$ has a direct product decomposition, this surjective K_v-algebra homomorphism maps onto each $(LM)_w$, for $w|v$. Since the left hand side is isomorphic to $K_v^{[L:K][M:K]}$, $(LM)_w$ must also be isomorphic to K_v^a for some a. The fact that this is a K_v-algebra isomorphism means $a = 1$. Thus, v is a totally split place.

1.3. Polynomial Splitting.

Let L be the splitting field of $f(x)$. Then L/K is separable, and $L = K(\theta)$ for some θ. For $\mathfrak{p} \in \mathcal{O}_K$ not dividing the conductor of $\mathcal{O}_K[\theta]$ (this applies to all but finitely many $\mathfrak{p}$), by the theorem relating primes above $\mathfrak{p}$ to irreducible factors of $f \pmod{\mathfrak{p}}$, for the $\mathfrak{p}$ such that $f \pmod{\mathfrak{p}}$ splits, $\mathfrak{p}$ also splits completely. Thus, all but finitely $\mathfrak{p}$ split, so their density is 1. Hence $[L:K] = 1$.

2. Proof of Hasse-Minkowski Theorem

Theorem. *Let K be a global field and f a non-degenerate quadratic form in n variables over k which represents 0 in k_v for each prime v of k. Then f represents 0 in k.*

We use the following observations

1. any quadratic form can be brought into diagonal form,
2. if a form represents 0, it represents any element of the field.
3. $cX_1^2 - g(X_2, ..., X_n)$ represents 0 if and only if g represents c.

2.1. $n = 1$.

One-variable forms do not represent 0.

2.2. $n = 2$. We may bring any two variable form to the form $X^2 - bY^2$. We claim this represents 0 if and only if $b \in (K^\times)^2$. The if is clear. For the only if, note that if $Y = 0$, then $X = 0$, so we have a contradiction. Then $Y \neq 0$, and $b = (X/Y)^2$.

Now we prove that b is a square globally if and only if it is a square everywhere locally. The only work to be done is in the reverse direction. Suppose $L = K(\sqrt{b})$ is a non-trivial abelian extension. Then infinitely many primes do not split completely (result of Cassels'). At such places v, $L \otimes_k K_v \cong L_w$, where w is the unique place extending v. Thus L_v is quadratic, so b is not a square of $K_v^\times$. This proves the $n = 2$ case.

2.3. $n = 3$. Bring f to the diagonal form $X^2 - bY^2 - cZ^2$. We claim that f represents 0 if and only if c is a norm from $K(\sqrt{b})$. If this is the case, then f represents 0 globally if and only if c is a global norm if and only if c is everywhere a local norm if and only if f represents 0 everywhere locally.

Now suppose $c = x_0^2 - by_0^2$ is a norm. Then $(x_0, y_0, 1)$ is a solution to $f = 0$. On the other hand, if $Z = 0$, then $X^2 - bY^2 = 0$. This has a solution if and only if b is a square. If b is not, then $Z \neq 0$, and we can divide by Z, showing that c is a norm.

2.4. $n = 4$. Bring f to the form $X^2 - bY^2 - cZ^2 + acT^2$. By exercise 4.4, which is done in Cassels-Frohlich, this represents 0 if and only if $g = X^2 - bY^2 - cZ^2$ represents 0 over $K(\sqrt{ab})$. This reduces the $n = 4$ case to $n = 3$.

2.5. $n \geq 5$. Write $f = aX_1^2 + bX_2^2 - g(X_3, ..., X_n)$. Let $h = aX_1^2 + bX_2^2$. Then $f = h - g$ represents 0 over every K_v. So for each v, there is an a_v that h, g both represent.

Exercise 4.5 guarantees that $g(X_3, X_4, X_5, 0, ..., 0)$ represents 0 in K_v for all but finitely many v. Call this collection of finitely many places S. For $v \in S$, suppose we can construct $(x_1, x_2) \in K \times K$ such that $c := h(x_1, x_2)$ and $c/a_v \in (K_v^\times)^2$. So $c = a_v \alpha_v^2$ for some α_v. Now consider the form $cY^2 - g$. g represents a_v and so does cY^2 (take $Y = 1/\alpha_v^2$). Thus, g represents c.

For $v \notin S$, we knew g represents c. This shows g represents c for $v \in S$. Thus, by induction, g represents c globally. By construction, h represents c globally. Thus, $f = h - g$ represents 0.

To complete the proof, we give the construction of c. Since $a_v(K_v^\times)^2$ is open, and so $h^{-1}(a_v K_v^{\times 2}) \subset K_v \times K_v$ is open. By approximation, we can find $(x_1, x_2) \in K \times K$ that are in this open set for every $v \in S$. Let $c := h(x_1, x_2)$.

3. Representability by $x^2 + dy^2$

Let $d > 1$ be a square-free integer with $d \equiv 1 \pmod 4$. Let p be a prime not dividing $2d$.

3.1. **Representation of Primes over $\mathbb{Z}$.** Let $K = \mathbb{Q}(\sqrt{-d})$. We show that $p = x^2 + dy^2$ if and only if p splits completely in $H_K/\mathbb{Q}$, where H_K is the Hilbert class field of K. We start by showing that $p = x^2 + dy^2$ if and only if p splits in $K/\mathbb{Q}$ into two principal primes. If $p = x^2 + dy^2 = (x + y\sqrt{-d})(x + y\sqrt{-d})$. These two factors will be different; otherwise, p is ramified, and divides the discriminant of K which is $2d$, a contradiction. Now suppose $(p) = (\alpha)(\beta)$. The Galois actions permutes the prime ideals, so $(\beta) = (\overline{\alpha})$. Thus $p = u\alpha\overline{\alpha} = uN(\alpha)$. Then u is rational, so $u = \pm 1$, and positivity requires $u = 1$. Thus $p = N(\alpha)$. Finally, by the previous homework, a prime of K splits completely in H_K if and only if they are principal.

By Chebotarev, the density of primes splitting in $H_K/\mathbb{Q}$ is $1/[H_K : \mathbb{Q}]$. Since $[H_K : \mathbb{Q}] = [H_K : K][K : \mathbb{Q}] = 2|\mathrm{Gal}(H_K/K)| = 2h_K$, by the previous global class field theory HW.

3.2. $d = 5$**.** If $p = x^2 + 5y^2$, then p splits completely in $H_K/\mathbb{Q}$. By previous homework, we have $H_K = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. Since p splits, if we complete at any prime $\mathfrak{p}$ above p we see that $(H_K)_{\mathfrak{p}} = \mathbb{Q}_p(\sqrt{-5}, \sqrt{-1}) = \mathbb{Q}_p$, for instance by looking at $H_K \otimes \mathbb{Q}_p$. This means $-5, -1$ are squares modulo p.

Clearly, $p = 2$ cannot be represented. For $p \neq 2$, -1 being a square means $p \equiv 1 \pmod 4$. By using quadratic reciprocity, we can deduce $p \equiv 0, 1, 4 \pmod 5$. By CRT, this means $p = 5$, $p \equiv 1 \pmod{20}$, or $p \equiv 9 \pmod{20}$.

3.3. **Representability of Primes over $\mathbb{Q}$.** We show $p = x^2 + dy^2$, $x, y \in \mathbb{Q}$ if and only if the following conditions hold.

(1) $p \in N_{\mathbb{Q}_2(\sqrt{-d})/\mathbb{Q}_2}\mathbb{Z}_2[\sqrt{-d}]^\times$,
(2) $p \in (\mathbb{Z}_l^\times)^2$ for all primes $l|d$,
(3) p splits in $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$.

Begin with the forward direction. Since p is a norm, it is everywhere a local norm, particularly at 2. Since $p \neq 2$, the valuation of $v(p)$ in this case is 0. Moreover, if $v(x) \neq v(y)$, then $v(x), v(y) \geq 0$, so x, y are integral. If $v(x) = v(y)$, then it must be that $v(x) = v(y) = 0$, so x, y are again integral.

For (2), notice again that p is a local norm at $l|d$. If v is the valuation for $\mathbb{Q}_l$, then $v(p) = 0$. Just as before, we can conclude that if $v(x^2) \neq v(dy^2)$, then $v(x^2), v(dy^2) \geq 0$. Otherwise, they are both equal to 0. This allows us to reduce modulo l, obtaining $x^2 \equiv p \pmod l$. Since $p \not\equiv 0 \pmod l$, we can lift this to a solution in $\mathbb{Z}_l$ via Hensel's lemma.

Finally, suppose $p = (a'/e')^2 + d(b'/f')^2$, for $a', b', e', f' \in \mathbb{Z}$. If $c = [e', f']$, we can write $c^2p = a^2 + db^2$ for $a, b, c \in \mathbb{Z}$. Moreover, c, which is the least common multiple of the denominators, is the smallest integer that clears denominators. This allows us to claim that p does not divide b. Otherwise, $p|a, b, c$, and we can obtain a smaller such c. Then modulo p, $-d \equiv (a/b)^2 \pmod p$, so $x^2 + d$ splits modulo p, so p splits.

To prove the reverse direction, we will use (1)-(3) to show that these imply that p is everywhere a local norm. Clearly, (1) and (2) imply p is a local norm at 2 and all l dividing d. Since p splits in $\mathbb{Q}(\sqrt{-d})$, completing at a prime above p yields $\mathbb{Q}_p(\sqrt{-d}) = \mathbb{Q}_p$, so p is a norm above p. Now take $l \nmid 2dp$. Then $\mathbb{Q}_l(\sqrt{-d})/\mathbb{Q}_l$ is unramified, and the norm map is surjective on units, so p is a norm over l. Thus, p is a global norm.

3.4. **Local Norms Imply Splitting.** Suppose (1) and (2) hold, we will show that (3) holds. From (1), we obtain $p = a^2 + db^2$ for $a, b \in \mathbb{Z}_2$. Reducing modulo 4 gives us $p \equiv a^2 + b^2 \equiv 1 \pmod 4$, so -1 is a square modulo p. If $d = l_1, ..., l_r$, we have that

$$\left(\frac{-d}{p}\right) = \prod_i \left(\frac{l_i}{p}\right),$$

where we have used the fact that -1 is a square modulo p. Finally, (2) and quadratic reciprocity, along with the fact that $p \equiv 1 \pmod 4$, shows that all these Legendre symbols are 1. Thus,

$$\left(\frac{-d}{p}\right) = 1,$$

implying (3).